(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 672 402**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **91 01268**

(51) Int Cl[5] : G 06 F 7/58

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 05.02.91.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 07.08.92 Bulletin 92/32.

(56) **Liste des documents cités dans le rapport de recherche** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *Société Anonyme dite GEMPLUS CARD INTERNATIONAL* — FR.

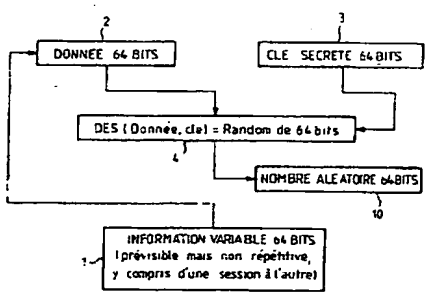
(72) **Inventeur(s)** : Geronimi François Cabinet Ballot-Schmit et Viricel Gilles.

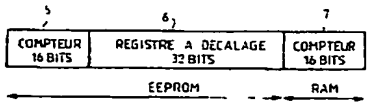
(73) **Titulaire(s)** :

(74) **Mandataire** : Cabinet Ballot-Schmit.

(54) Procédé et dispositif pour la génération de nombres pseudo-aléatoires uniques.

(57) Le procédé consiste à inscrire (1, 2) dans une zone déterminée de la mémoire non volatile d'une carte à mémoire à microcircuit une information de valeur déterminée et non répétitive à chaque génération d'un nombre aléatoire et à convertir (3, 4) cette information en une information ayant la forme d'un nombre pseudo-aléatoire en programmant l'unité de traitement au moyen d'un programme de cryptage de l'information standard, type DES.
Applications: cartes à mémoire.





FR 2 672 402 - A1

BNSDOCID: <FR__2672402A1_I_>

PROCEDE ET DISPOSITIF POUR LA GENERATION DE NOMBRES PSEUDO-ALEATOIRES UNIQUES

La présente invention concerne un procédé et un dispositif pour la génération de nombres pseudo-aléatoires uniques.

Elle s'applique notamment à la réalisation de cartes à microcircuits dites à puces utilisables dans tout système où l'accès à des informations ou à des services est sévèrement contrôlé. Il s'agit notamment des systèmes distributeurs de monnaie fiduciaire, du domaine des systèmes de télévision à péage ; des systèmes pour la distribution d'essence ou de fuel domestique ; des systèmes pour l'accès aux banques de données etc...

Dans les cartes à mémoire à microprocesseur qui sont utilisées dans les domaines précédents, l'accès à des informations ou à des services est sévèrement contrôlé. On utilise pour cela des mots de passe. Ces mots de passe sont de plus en plus souvent transmis en les cryptant par un code pseudo-aléatoire fourni par un générateur à structure programmée ou éventuellement câblée. Dans les cartes à mémoire à base de microprocesseurs, il n'existe dans l'état de la technique que des générateurs matériels (basé sur des phénomènes physiques) ou des générateurs logiciels basé sur des propriétés mathématiques et déjà utilisés dans le monde informatique traditionnel. Ces deux principes ne peuvent pas garantir l'unicité des nombres générés ce qui présente un inconvénient majeur de sécurité en matière de cryptographie moderne.

Si cette solution présente l'avantage de ne pas renseigner les fraudeurs sur les mots de passe

BNSDOCID: <FR__2672402A1_I_>

utilisés, elle laisse en effet la possibilité à ces derniers de recopier les mots de passe cryptés transmis qui, de par leur défaut d'unicité, peuvent toujours être réutilisés pour donner l'accès aux informations ou services pour lesquels la carte est dédiée. En effet, il suffit alors de renouveler l'expérience de manière à retrouver une valeur déjà utilisée et ainsi frauder le système.

Par ailleurs, la production de nombre aléatoire unique se heurte aux possibilités technologiques de réécriture dans des mémoires non volatiles. Chaque cellule ne peut en effet être réécrite plus de 10.000 fois. Le but de l'invention est de pallier les inconvénients précités.

A cet effet, l'invention a pour objet un procédé pour la génération de nombres pseudo-aléatoires uniques dans une carte à mémoire à microcircuits comportant au moins une mémoire non volatile réinscriptible (EEPROM) couplée à un organe de traitement de données, caractérisé en ce qu'il consiste

- à inscrire dans une zone déterminée de la mémoire, une information de valeur déterminée et non répétitive à chaque génération d'un nombre aléatoire et,
- à convertir cette information en une information ayant la forme d'un nombre pseudo-aléatoire en lui faisant subir dans l'organe de traitement de données un programme de cryptage de type DES.

Elle a également pour objet un dispositif pour la mis en oeuvre du procédé.

L'invention a en outre pour principal avantage de permettre, en utilisant un compteur qui comporte un registre à décalage, d'obtenir un nombre de tirages très élevé de nombres aléatoires comparativement au nombre de cycles d'effacement/écriture autorisés dans la mémoire

BNSDOCID: <FR___2672402A1_I_>

non volatile équipant habituellement les cartes à mémoire. Ainsi, malgré un nombre d'effacement/écriture limité à 10.000 par la technologie actuelle des mémoires non volatiles, encore connues sous la désignation EEPROM, il est possible, grâce à l'invention, de générer dans le pire des cas 320.000 valeurs différentes et dans le meilleur des cas 21 milliards, en utilisant un espace mémoire EEPROM très réduit de 64 bits.

D'autres caractéristiques et avantages de l'invention apparaîtront ci-après à l'aide de la description qui suit faite en regard des dessins annexés qui représentent :

Figure 1 : un mode d'exécution du procédé selon l'invention mis sous la forme d'un organigramme.

Figure 2 : un format d'un mot d'information utilisable pour la mise en oeuvre du procédé selon l'invention représenté par l'organigramme de la figure 1.

Dans sa définition la plus générale, une carte à mémoire pour l'application du procédé selon l'invention comporte, de façon connue et non représentée, un dispositif de mémorisation et un organe de traitement formé normalement par un microprocesseur ou tout dispositif équivalent, couplés l'un à l'autre par un bus de données et d'adresses. Ce bus assure également la liaison du microcircuit de la carte ainsi formée, avec des dispositifs d'écriture et de lecture extérieurs à la carte. Le dispositif de mémorisation comporte généralement une mémoire non volatile, de type EPROM ou EEPROM, dans laquelle sont enregistrés des microprogrammes nécessaires au fonctionnement de l'organe de traitement et normalement une mémoire vive volatile de type RAM. Cette dernière sert pour la mémorisation temporaire des données et des instructions

BNSDOCID: <FR___2672402A1_I_>

spécifiques de l'application en cours avec la carte à mémoire. Dans la mémoire non volatile sont rangés, par exemple, d'une part le code secret identifiant le titulaire de la carte, avec éventuellement un programme de chiffrement pour l'obtention d'une signature calculée sur la base du code secret et, d'autre part, des instructions du programme d'utilisation lui-même.

Le procédé selon l'invention dont les étapes 1 à 4 sont représentées schématiquement sur l'organigramme de la figure 1 consiste, chaque fois qu'un nombre aléatoire 10 est à produire, à calculer suivant les étapes 1 et 2, à partir d'une donnée 1 d'information déterminée (de longueur N = 64 bits par exemple), une nouvelle donnée 2 de même longueur N, mais dont la valeur ne pourra plus à nouveau être générée lors d'une requête ultérieure de nouvelle donnée 2. Une fois transformée, la donnée 2 est à l'étape 4 associée à une clef secrète 3 comportant un même nombre de bits, par un algorithme de calcul communément connu sous l'abréviation anglo-saxonne DES de "Data Encryption Standard" et dont une description peut être trouvée dans les brochures des normes FIPS des "Federal Information Processing Standards" des Etats-Unis d'Amérique.

La supériorité de l'algorithme d'association DES sur les autres algorithmes d'association est qu'il permet d'obtenir pour chaque clef secrète constante 3 de longueur de N bits, les 2^N combinaisons possibles du résultat en garantissant toujours le caractère non prévisible du nombre aléatoire 10, c'est-à-dire, d'obtenir toujours des nombres aléatoires différents 10. Ceci est obtenu à partir des 2^N combinaisons possibles de la donnée en entrée. Mais le fait que la clé ait une longueur de N bits n'a rien à voir avec le fait qu'il y ait 2^N combinaisons différentes sur le résultat. Ceci

BNSDOCID: <FR___2672402A1_I_>

est lié au fait que la donnée en entrée à une longueur de N bits. Par exemple, les caractéristiques de DES indiquent que pour une clef secrète constante, les 2^{64} combinaisons possibles de la donnée balaient les 2^{64} combinaisons possibles du résultat ce qui garantit, en plus du caractère non prévisible du nombre aléatoire (lié aux performances de DES), la propriété de toujours obtenir des nombres aléatoires différents. Dans l'invention, on disposera ainsi d'une clef secrète constante 3.

Pour obtenir ce résultat, chaque donnée 2 d'information variable est structurée de la façon qui est représentée à la figure 2. Son format comporte trois zones, une première zone 5 de capacité égale par exemple à 16 bits représente les états pris par un premier compteur, une deuxième zone 6 de capacité égale par exemple à 32 bits représente les états d'un registre à décalage et, une troisième zone 7 de capacité égale par exemple à 16 bits représente les états d'un deuxième compteur. Les première et deuxième zones 5 et 6 sont alors situées dans une mémoire non volatile de la carte alors que la zone 7 est située en mémoire vive. Selon l'invention, le contenu des trois zones est considéré comme équivalent à celui qui serait donné par un compteur de N bits qui serait incrémenté à chaque demande de calcul. Cette information est donc prévisible mais est toujours différente des valeurs précédentes. Le stockage en mémoire EEPROM des données des zones 5 et 6 permet de conserver les valeurs de leur contenu lorsque la tension d'alimentation de la carte est supprimée. Cette solution permet d'obtenir un nombre maximum de nombres aléatoires très supérieur aux 10.000 autorisés par la technologie EEPROM.

La zone 6, qui est organisée en registre à

BNSDOCID: <FR__2672402A1_I_>

décalage, permet d'obtenir un nombre maximum de nombre aléatoires. Pour cela, à chaque nouveau calcul ou session, un bit de valeur 1 est chargé à la dernière position de poids le plus faible du registre qui est encore à 0. Lorsque 32 demandes de calcul, correspondant à la mise à 1 des 32 bits du registre 6 à décalage, sont effectuées, le calcul suivant remet à zéro le registre à décalage représenté par la zone 6. Lorsque les 32 calculs ont été réalisés, le registre à décalage est à la valeur FFFFFFFFH bien que chaque bit n'ait été écrit qu'une seule fois. On obtient ainsi 32 valeurs différentes en ne consommant qu'une seule écriture pour chaque cellule. A chaque effacement de ce registre de 32 bits, le compteur de 16 bits de la zone 5 en EEPROM sera incrémenté ce qui en définitive permet d'obtenir, 32 X 10000 = 320000 valeurs imprévisibles et non répétitives pour la donnée 2 (sans qu'aucun des bits manipulés en EEPROM ne soit effacé/écrit plus de 10000 fois). Pour obtenir une plus grande quantité de valeurs (hors pire cas), il suffit d'adjoindre à cette variable de 48 bits en EEPROM, un compteur 7 de 16 bits en RAM qui sera incrémenté à chaque calcul dans une même session.

La zone 7 située en mémoire RAM permet donc d'augmenter le nombre des valeurs précédentes en augmentant, de manière similaire au compteur matérialisé par la zone 5, le contenu du compteur matérialisé par la zone 7 à chaque nouveau calcul dans une même session. S'il arrive dans une même session que ce compteur déborde, c'est-à-dire que son contenu dépasse ici 65536 valeurs, on peut modifier le contenu du registre à décalage matérialisé par la zone 6 de la mémoire EEPROM comme si une nouvelle session commençait. Dans ce cas, on met à 1 un autre des bits de ce registre 6.

Au total, cette disposition permet en concaténant,

BNSDOCID: <FR___2672402A1_I_>

c'est-à-dire en juxtaposant les 48 bits en EEPROM aux 16 bits situés en mémoire RAM, d'obtenir 320.000 X 65536 soit environ 21 milliards de valeurs imprévisibles et non répétitives par la mise en oeuvre d'un calcul de nombres aléatoires en utilisant l'algorithme DES précédemment cité.

Par sécurité, on associe au compteur 5 de 16 bits en EEPROM un compteur-image en EEPROM. Ce compteur-image contient toujours la même valeur que le véritable compteur et est utilisé dans le cas où la valeur du compteur est détruite (arrachage de la carte lorsque le compteur vient d'être effacé pour en modifier la valeur). Il n'est pas nécessaire de prévoir la même chose pour le registre à décalage car celui-ci n'est effacé que pour sa remise à zéro.

La structure du compteur ainsi utilisée (comprenant un registre à décalage) permet d'obtenir un nombre de tirages très élevé comparativement au nombre de cycles d'effacement/écriture (mise à jour) autorisé dans la mémoire non volatile. Ainsi, malgré un nombre d'effacement/écriture limité à 10000 par la technologie EEPROM, on arrive à générer dans le pire des cas 320.000 valeurs différentes et dans le meilleur des cas 21 milliards.

BNSDOCID: <FR___2672402A1_I_>

REVENDICATIONS

1. Procédé pour la génération de nombres pseudo-aléatoires uniques dans une carte à mémoire à microcircuits comportant au moins une mémoire non volatile réinscriptible (EEPROM) couplée à un organe de traitement de données caractérisé en ce qu'il consiste,

- à inscrire (1,2) dans une zone déterminée de la mémoire, une information de valeur déterminée et non répétitive à chaque génération d'un nombre aléatoire et,

- à convertir (3,4) cette information en une information ayant la forme d'un nombre pseudo-aléatoire en lui faisant subir dans l'organe de traitement de données un programme de cryptage de type DES.

2. Procédé selon la revendication 1, caractérisé en ce que l'information de valeur déterminée et non répétitive est inscrite dans une mémoire EEPROM de la carte.

3. Procédé selon la revendication 2, caractérisé en ce que l'information de valeur déterminée et non répétitive est structurée suivant au moins deux zones, une première zone (6) pour écrire de façon systématique au moins un nouveau bit chaque fois qu'un nombre pseudo-aléatoire est généré par la carte, et une deuxième zone (5) de comptage pour totaliser le nombre de fois où la première zone a été totalement écrite.

4. Procédé selon la revendication 3, caractérisé en ce qu'il consiste à structurer l'information de valeur déterminée et non répétitive en lui rajoutant une troisième zone (7) de comptage pour totaliser le nombre de fois où, dans une même session, un nombre pseudo-aléatoire a été généré.

BNSDOCID: <FR__2672402A1_J_>

5. Procédé selon la revendication 4, caractérisé en ce que les première et deuxième zones (6, 5) sont mémorisées dans une mémoire non volatile de la carte et en ce que la troisième zone (7) est mémorisée dans une mémoire volatile de la carte.

6. Procédé selon la revendication 3, caractérisé en ce qu'on réserve une troisième zone pour servir d'image du résultat du comptage totalisé dans la deuxième zone.

7. Dispositif pour la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il est formé par une carte à microcircuit comportant une unité de traitement couplée à une mémoire non volatile et à une mémoire volatile.

BNSDOCID: <FR__2672402A1_I_>

FIG_1

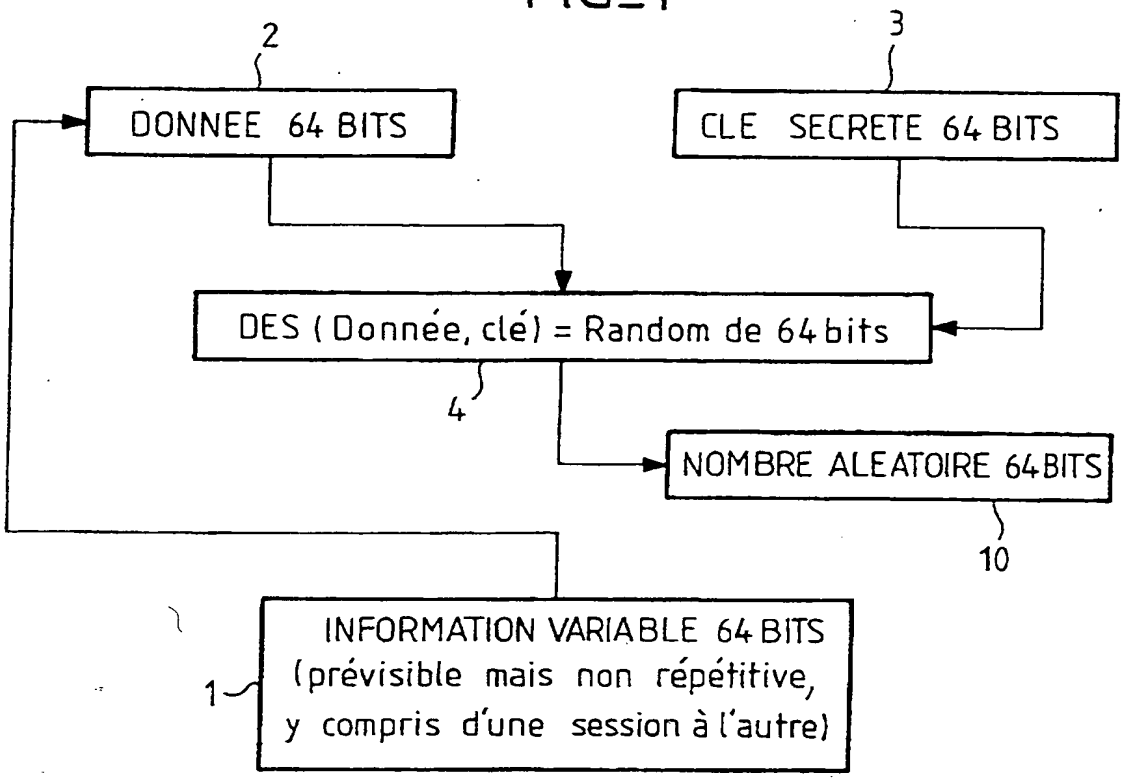
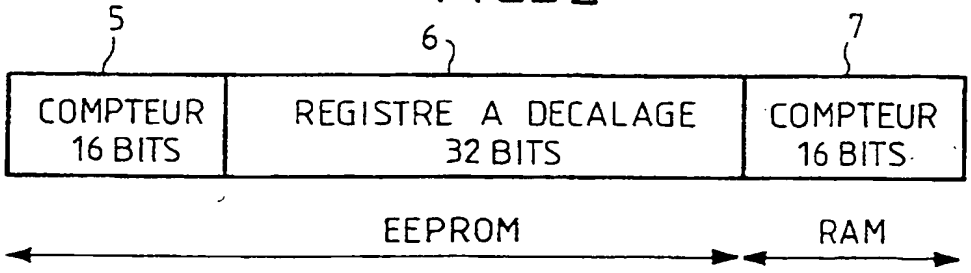


FIG_2



BNSDOCID: <FR__2672402A1_I_>

REPUBLIQUE FRANÇAISE

2672402

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FR 9101268
FA 454010

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y	EP-A-0386677 (SIEMENS) * le document en entier *	1, 2, 7
Y	EP-A-0284133 (TRT) * le document en entier *	1, 2, 7
A	US-A-4802217 (MICHENER) * le document en entier *	1

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G06F

Date d'achèvement de la recherche	Examinateur
05 SEPTEMBRE 1991	DURAND, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0413)

BNSDOCID: <FR___2672402A1_I_>